PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-227669

(43)Date of publication of application : 12.08.2004

(51)Int.Cl. G11B 20/10

(21)Application number : 2003-014219

(22)Date of filing : 23.01.2003

(71)Applicant : SHINANO KENSHI CO LTD

(72)Inventor : HANDA YUJI

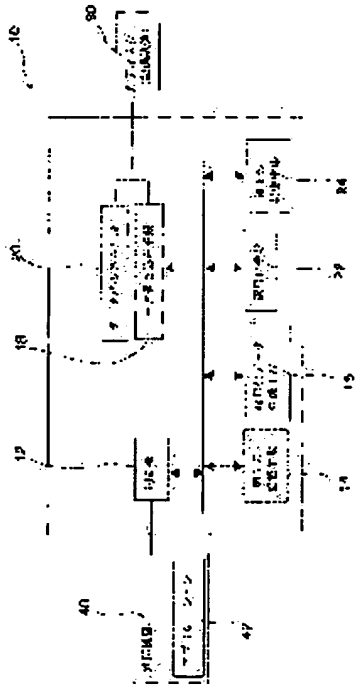
TAKAHASHI KAZUKI

(54) DATA RECORDER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a recorder capable of encrypting the data on hardware and recording the encrypted data on a recording medium without depending upon an application.

SOLUTION: A data recorder 10 consists of: an inputting means 42 for operation; a storing means 14; an encrypted data generating means 16 for encrypting the data on the basis of a password determined by a user; a data write means 18 for writing the data on the recording medium 30; a data read means 20 for reading the data on the recording medium 30; and a control part 12 for making them cooperate. In a data writing mode, the control part 12 stores the data from an external device into the storing means 14, makes the encrypted data generating means 16 generate encrypted data from the data stored in the storing means 14 on the basis of the password set by the user, and performs processing that makes the data write means 18 record the encrypted data on the recording medium 30.



LEGAL STATUS

[Date of request for examination] 26.11.2003

[Date of sending the examiner's decision of 11.07.2006

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-227669
(P2004-227669A)
(43)公開日　平成16年8月12日(2004.8.12)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5D044
	G11B 20/10	301A	

審査請求 有　請求項の数 12　OL　（全 13 頁）

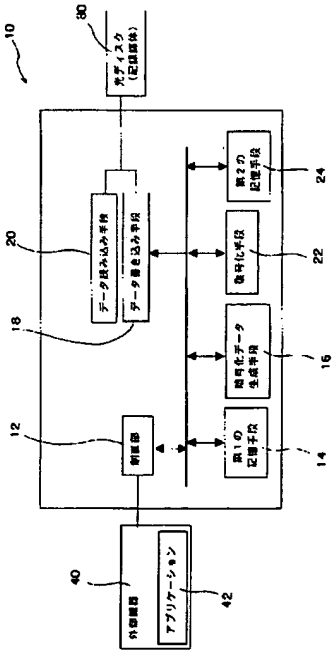
(21)出願番号　特願2003-14219(P2003-14219)
(22)出願日　平成15年1月23日(2003.1.23)

(71)出願人　000106944
シナノケンシ株式会社
長野県小県郡丸子町大字上丸子１０７８
(74)代理人　100077621
弁理士　綿貫　隆夫
(74)代理人　100092819
弁理士　堀米　和春
(72)発明者　半田　雄士
長野県上田市中央６－１５－２６　シナノケンシ株式会社電子機器事業部内
(72)発明者　高橋　和樹
長野県上田市中央６－１５－２６　シナノケンシ株式会社電子機器事業部内

Fターム(参考)　5D044 AB05 AB07 BC04 CC04 DE50 GK17

(54)【発明の名称】データ記録装置

(57)【要約】
【課題】アプリケーションに頼らず、ハードウェアにおいてデータを暗号化して記録媒体に記録可能な記録装置を提供する。
【解決手段】操作用入力手段４２と、記憶手段１４と、ユーザが決定したパスワードを基にして、データを暗号化する暗号化データ生成手段１６と、記録媒体３０にデータを書き込むデータ書き込み手段１８と、記録媒体３０のデータを読み取るデータ読み取り手段２０と、これらを協働させる制御部１２とで構成され、データ書き込み時では、制御部１２が、外部機器からのデータを記憶手段１４に記憶させ、暗号化データ生成手段１６に、ユーザが設定したパスワードに基づいて、記憶手段１４に記憶されたデータから暗号化データを生成させ、データ書き込み手段１８により、暗号化データを記録媒体３０に記録させる処理をすることを特徴とするデータ記録装置１０である。
【選択図】　図１



【特許請求の範囲】
【請求項１】
操作用入力手段と、
単数または複数の記憶手段と、
ユーザにより設定され、前記操作用入力手段から入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化データ生成手段と、
記録媒体にデータを書き込むデータ書き込み手段と、
記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、
これらの各手段を協働させる制御部とにより構成され、
データ書き込み時においては、
前記制御部が、
外部機器から送信されたデータを１の記憶手段に一時記憶させ、
前記暗号化データ生成手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、前記１の記憶手段に一時記憶されたデータから所定のアルゴリズムにより暗号化データを生成させ、
前記データ書き込み手段により、該暗号化データを前記記録媒体に記録させる処理をすることを特徴とするデータ記録装置。
【請求項２】
操作用入力手段と、
単数または複数の記憶手段と、
記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、
前記操作用入力手段から入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、
これらの各手段を協働させる制御部とにより構成され、
データ読み取り時においては、
前記制御部が、
前記読み取り手段に、前記記録媒体から前記暗号化データを読み取らせ、
前記復号化手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、所定のアルゴリズムにより前記暗号化されたデータを復号化させる処理をすることを特徴とするデータ記録装置。
【請求項３】
操作用入力手段と、
単数または複数の記憶手段と、
ユーザにより設定され、前記操作用入力手段から入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化データ生成手段と、
記録媒体にデータを書き込むデータ書き込み手段と、
記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、
前記操作用入力手段から入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、
これらの各手段を協働させる制御部とにより構成され、
データ書き込み時においては、
前記制御部が、
外部機器から送信されたデータを１の記憶手段に一時記憶させ、
前記暗号化データ生成手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、前記１の記憶手段に一時記憶されたデータから所定のアルゴリズムにより暗号化データを生成させ、
前記データ書き込み手段により、該暗号化データを前記記録媒体に記録させる処理をして、
データ読み取り時においては、
前記制御部が、

前記読み取り手段に、前記記録媒体から前記暗号化データを読み取らせ、
前記復号化手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、所定のアルゴリズムにより前記暗号化されたデータを復号化させる処理をすることを特徴とするデータ記録装置。
【請求項４】
他の記憶手段には、補助パスワードがあらかじめ記憶されていて、
前記制御部は、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに、前記補助パスワードを付加した後に、前記暗号化データ生成手段に暗号化データを生成させる処理をすることを特徴とする請求項１または３に記載のデータ記録装置。
【請求項５】
前記他の記憶手段には、補助パスワードがあらかじめ記憶されていて、
前記制御部は、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに前記補助パスワードを付加した後に、前記復号化手段に暗号化データを復号させる処理をすることを特徴とする請求項２または３に記載のデータ記録装置。
【請求項６】
前記操作用入力手段は、前記他の記憶手段に、前記ユーザにより設定され、前記操作用入力手段から入力されたパスワードまたはパスワードおよび補助パスワードを記憶させるか否かを選択可能に設定されていることを特徴とする請求項１乃至５いずれか一項に記載のデータ記録装置。
【請求項７】
前記補助パスワードは当該データ記録装置に関する情報であることを特徴とする請求項４乃至６いずれか一項に記載のデータ記録装置。
【請求項８】
前記補助パスワードは複数個設定可能であることを特徴とする請求項４乃至７いずれか一項に記載のデータ記録装置。
【請求項９】
前記他の記憶手段にはハッシュ関数が記憶されていて、
前記制御部が、データ書き込み時において、前記ユーザにより設定され、前記操作用入力手段から入力されたパスワードまたは、前記ユーザにより前記操作用入力手段から入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、
前記暗号化データ生成手段により暗号化データを生成させる処理をすることを特徴とする請求項１、３、４、７、８いずれか一項に記載のデータ記録装置。
【請求項１０】
前記他の記憶手段にはハッシュ関数が記憶されていて、
前記制御部が、データ読み取り時において、前記ユーザにより設定され、前記操作用入力手段から入力されたパスワードまたは、前記ユーザにより前記操作用入力手段から入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、
前記復号化手段により暗号化データを復号させる処理をすることを特徴とする請求項２、３、５、７、８いずれか一項に記載のデータ記録装置。
【請求項１１】
前記操作用入力手段は、前記ユーザにより設定されて入力されたパスワードまたは、前記ユーザにより設定されて入力されたパスワードおよび前記補助パスワードを、前記ハッシュ関数によりハッシュ化した後に、前記他の記憶手段に記憶させるか否かを選択可能に設定されていることを特徴とする請求項９または１０に記載のデータ記録装置。
【請求項１２】
前記記録媒体は、リムーバブルであることを特徴とする請求項１乃至１１いずれか一項に記載のデータ記録装置。
【発明の詳細な説明】

【０００１】
【発明の属する技術分野】
本発明はデータ記録装置に関し、より詳細には、暗号化および復号化処理に必要なパスワードを任意に設定することが可能なデータ記録装置に関する。
【０００２】
【従来の技術】
データに機密性を持たせる方法として、暗号化アプリケーションによるデータの暗号化が一般的に用いられている。データの暗号化は、当該データをアプリケーションに搭載されている所定のアルゴリズムによりおこなわれる。このようにして暗号化されたデータは、予め設定されているパスワードを入力し、暗号化アルゴリズムに対応した復号化アルゴリズムにより復号（解読）した後に、データが実際に使用可能になる。
近年においては、アプリケーションで行っていたデータの暗号化および復号化処理を記録装置に行わせることを想定した発明が特許文献１に記載されている。
【０００３】
【特許文献１】
特開平１－２２７２７２号公報
【０００４】
【発明が解決しようとする課題】
しかしながら、特許文献１におけるデータ記録装置においては、データを暗号化する際において最も重要であるパスワードについては何ら記載されておらず、パスワードが設定されてなく、単純に平文データを所定のアルゴリズムで暗号化処理しているものと思われる。
したがって、特許文献１により生成された暗号化データは、暗号化したデータ記録装置と同種類のものを用いれば、誰でも復号（平文化）することができてしまうため、データの機密性が確保できなくなってしまうといった課題がある。
【０００５】
また、アプリケーションで平文データを暗号化処理したり、暗号化データを復号化する作業をさせると、パソコンのＣＰＵに負荷をかけてしまうため、暗号化処理や復号化処理を行っている間は、他の作業が円滑に行うことができなくなってしまう等の課題もある。
【０００６】
本発明の目的は、データを暗号化し、かつ、復号化する処理手段を記録装置に搭載し、さらには、暗号化したデータを復号する際のパスワードの設定をユーザーが任意に行うことを可能にしたデータ記録装置を提供することにある。
【０００７】
【課題を解決するための手段】
本願発明は、データを暗号化し、かつ、復号化する処理手段を記録装置に搭載し、さらには、暗号化したデータを復号する際のパスワードの設定をユーザーが任意に行うことを可能にするため、以下の手段を有している。
すなわち、操作用入力手段と、単数または複数の記憶手段と、ユーザにより設定され、前記操作用入力手段から入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化データ生成手段と、記録媒体にデータを書き込むデータ書き込み手段と、記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、これらの各手段を協働させる制御部とにより構成され、データ書き込み時においては、前記制御部が、外部機器から送信されたデータを１の記憶手段に一時記憶させ、前記暗号化データ生成手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、前記１の記憶手段に一時記憶されたデータから所定のアルゴリズムにより暗号化データを生成させ、前記データ書き込み手段により、該暗号化データを前記記録媒体に記録させる処理をすることを特徴とするデータ記録装置である。
これにより、ユーザが任意のパスワードを設定することができるので、機密性を高めることができる。さらには、バックグラウンドで暗号化処理をすることができるので、アプリ

ケーションで暗号化している場合に比べ、パソコン等の外部機器の演算装置に負担をかけないため、データを暗号化している間にパソコン等で他の処理を行わせることが可能になるので、パソコン等の作業効率が向上する。

【０００８】

また、他の発明は、操作用入力手段と、単数または複数の記憶手段と、記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、前記操作用入力手段から入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、これらの各手段を協働させる制御部とにより構成され、データ読み取り時においては、前記制御部が、前記読み取り手段に、前記記録媒体から前記暗号化データを読み取らせ、前記復号化手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、所定のアルゴリズムにより前記暗号化されたデータを復号化させる処理をすることを特徴とするデータ記録装置である。

これによれば、ユーザが任意のパスワードを設定することができるので、パスワードの管理がしやすくなり、手軽に暗号化データを復号化することが可能になる。さらには、パソコン等の外部機器の演算装置に負担をかけないため、パソコン等の作業に対してバックグラウンドで復号化処理をすることができるので、暗号化データを復号化している間にパソコン等で他の処理を行わせることが可能になるのでパソコン等の作業効率が向上する。

【０００９】

また、さらに他の発明は、操作用入力手段と、単数または複数の記憶手段と、ユーザにより設定され、前記操作用入力手段から入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化データ生成手段と、記録媒体にデータを書き込むデータ書き込み手段と、記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、前記操作用入力手段から入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、これらの各手段を協働させる制御部とにより構成され、データ書き込み時においては、前記制御部が、外部機器から送信されたデータを１の記憶手段に一時記憶させ、前記暗号化データ生成手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、前記１の記憶手段に一時記憶されたデータから所定のアルゴリズムにより暗号化データを生成させ、前記データ書き込み手段により、該暗号化データを前記記録媒体に記録させる処理をして、データ書き込み時においては、外部機器から送信されたデータを前記１の記憶手段に一時記憶させ、前記暗号化データ生成手段に、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに基づいて、前記１の記憶手段に一時記憶されたデータから所定のアルゴリズムにより暗号化データを生成させ、前記データ書き込み手段により、該暗号化データを前記記録媒体に記録させる処理をすることを特徴とするデータ記録装置である。

これによれば、ユーザが任意のパスワードを設定することができるので、パスワードの管理がしやすくなり、手軽に暗号化データの作成ができると共に、暗号化されているデータを復号化することが可能になる。さらには、パソコン等の外部機器の演算装置に負担をかけないため、パソコン等の作業に対してバックグラウンドで復号化処理をすることができるので、暗号化データを復号化している間にパソコン等で他の処理を行わせることが可能になるのでパソコン等の作業効率が向上する。

【００１０】

また、他の記憶手段には、補助パスワードがあらかじめ記憶されていて、前記制御部は、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに、前記補助パスワードを付加した後に、前記暗号化データ生成手段に暗号化データを生成させる処理をすることも可能である。

これにより、暗号化するデータを復号処理する際における属性を付加させることが可能になる。またさらには、暗号化したデータを復号化処理する際におけるデータの機密性を向上させることが可能になる。

さらに、前記他の記憶手段には、補助パスワードがあらかじめ記憶されていて、前記制御部は、ユーザにより設定され、前記操作用入力手段から入力されたパスワードに前記補助

パスワードを付加した後に、前記復号化手段に暗号化データを復号させる処理をすることも可能である。
これによれば、属性を有する暗号化データを復号処理することが可能になる。
【００１１】
また、前記操作用入力手段は、前記他の記憶手段に、前記ユーザにより設定され、前記操作用入力手段から入力されたパスワードまたはパスワードおよび補助パスワードを記憶させるか否かを選択可能に設定されていることが好ましい。
これによれば、いちいちパスワードを設定しなくても済み、限られたワークグループ内での使用においては、グループ内での記憶装置の設定を一致させておけば、そのワークグループ内でしかデータを復号することができなくすることができるので、使い勝手が向上する。
【００１２】
さらにまた、前記補助パスワードは当該データ記録装置に関する情報であることが好ましい。
これにより、ユーザが設定した任意の文字列からなるパスワードに補助パスワードを組み合わせて鍵を形成し、暗号化データ生成手段により暗号化がなされることになるため、たとえ、ユーザが設定したパスワードを入手したとしても、暗号化データを復号処理させることができなくなるため好適である。
また、補助パスワードは複数設定することが可能であることが好ましい。
これにより、データの機密性をさらに向上させることが可能になる。
【００１３】
さらにまた、前記他の記憶手段にはハッシュ関数が記憶されていて、前記制御部が、データ書き込み時において、前記ユーザにより設定され、前記操作用入力手段から入力されたパスワードまたは、前記ユーザにより前記操作用入力手段から入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、前記暗号化データ生成手段により暗号化データを生成させる処理をすることが好ましい。
これによれば、ユーザが設定したパスワードの長短によるパスワードの強度のばらつきをなくし、均一のレベルにすることが可能になる。また、暗号化する際に用いる鍵の長さを一定にすることができるので、処理が容易に行うことができる。
また、前記他の記憶手段にはハッシュ関数が記憶されていて、前記制御部が、データ読み取り時において、前記ユーザにより設定され、前記操作用入力手段から入力されたパスワードまたは、前記ユーザにより前記操作用入力手段から入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、前記復号化手段により暗号化データを復号させる処理をすることが好ましい。
これによれば、ユーザが設定したパスワードの長短等によるパスワードの強度のばらつきをなくし、均一のレベルにすることが可能になる。また、暗号化や復号化する際に用いる鍵の長さを一定にすることができるので、処理を容易に行うことができる。
【００１４】
さらに、前記操作用入力手段は、前記ユーザにより設定されて入力されたパスワードまたは、前記ユーザにより設定されて入力されたパスワードおよび前記補助パスワードを、前記ハッシュ関数によりハッシュ化した後に、前記他の記憶手段に記憶させるか否かを選択可能に設定されていることがこのましい。
これにより、いちいちパスワードの設定が不要になるため、ある一定の範囲内（限られたユーザどうしの間）のみの記録装置の使用である場合には、記録装置の設定を一致させておけば、限られたユーザどうし間でのみ使用することが可能になる。
【００１５】
また、前記記録媒体は、リムーバブルであることが好ましい。
これによれば、データの供給先のデータ記録装置の規格が共通していれば、該データ記録装置の設定を供給元のデータ記録装置の設定に合わせることにより、暗号化したデータを生成した記録装置以外の記録装置においてもデータを復号することができるため、暗号化

データの使用が認められているユーザ間においては暗号化データの共有が容易になり、利便性が向上する。

【００１６】

【発明の実施の形態】

以下、本発明に係るデータ記録装置の好適な実施の形態を添付図面に基づいて詳細に説明する。

なお本発明は、本実施の形態に限定されるものではなく、発明の要旨を変更しない範囲において、各種の改変がなされても本発明の技術的範囲に属するのは言うまでもない。

【００１７】

（第１の実施の形態）

まず、本実施の形態におけるデータ記録装置の概要について図１を用いて説明する。本実施の形態においては、データ記録装置として光ディスク装置を用いることにする。図１は、暗号化機能を有する光ディスク装置の構成を示す説明図である。

本発明に係る暗号化機能を有する光ディスク装置１０は、パーソナルコンピュータ等の外部機器４０に設置され、外部機器４０から当該光ディスク装置１０を操作可能にする操作用入力手段であるアプリケーション４２と、パーソナルコンピュータ等の外部機器４０から送られてくる平文データを一時記憶する第１の記憶手段１４と、ユーザにより設定され、アプリケーション４２から入力されたパスワードを用いて、第１の記憶手段１４に一時記憶されている平文データを暗号化する暗号化データ生成手段１６と、暗号化データ生成手段１６により暗号化されたデータを記録媒体である光ディスク３０に書き込むデータ書き込み手段１８と、光ディスク３０に記録された暗号化データを読み取るデータ読み込み手段２０と、ユーザにより設定され、アプリケーション４２から再度入力されたパスワードを用いて、暗号化されているデータを復号する復号化手段２２と、これらを統括管理する制御部１２とにより概略が構成されている。

【００１８】

本実施の形態においては、光ディスク装置１０における暗号化データ生成手段１６と、復号化手段２２は、それぞれ別体であるとしているが、光ディスク装置１０に内蔵されているＣＰＵ等の制御部１２がこれらを統括する形態であっても良いのはもちろんである。

また、データ書き込み手段１８とデータ読み込み手段２０とについては、光ピックアップ（図示せず）にひとまとめにしてしまうのも、もちろん可能である。

【００１９】

明細書中における平文データとは、暗号化処理される前のデータであって、光ディスク３０の記録フォーマットさえ一致していれば他の光ディスク装置でもアクセスが可能なデータのことを指している。

【００２０】

アプリケーション４２は、パーソナルコンピュータ等の外部機器４０の図示しない記憶手段にインストールされていて、外部機器４０でアプリケーション４２を起動し、アプリケーション４２を操作することにより、光ディスク装置１０の制御部１２に各種のコマンドを送信することにより光ディスク装置１０の動作を制御することが可能である。

アプリケーション４２においては、光ディスク装置１０において平文データを暗号化処理した後にデータ書き込み手段１８が光ディスク３０に暗号化データを書き込むのか、平文データのままでデータ書き込み手段１８が光ディスク３０にデータを書き込むのかについて選択可能に設定されているので、ユーザは必要に応じてデータの記録態様を選択することができる。

【００２１】

暗号化処理をした後に暗号化データを光ディスク３０に記録する態様においては、アプリケーション４２においてさらに詳細に設定することが可能である。例えば、データを暗号化処理して光ディスク３０に記録した暗号化データを他の光ディスク装置では復号化処理することができないようにする設定や、同じグループ内においてのみ光ディスク３０に記録した暗号化データを復号化処理することができるようにする設定や、他の光ディスク装

置１０であっても光ディスク３０に記録した暗号化データを復号化することができるように,する設定があげられる。

【００２２】

ユーザがアプリケーション４２上において、データを暗号化データ生成手段１６により暗号化処理した後にデータ書き込み手段１８が光ディスク３０にデータを書き込むように選択した場合には、先に説明したように、暗号化処理されたデータの復号化処理の態様もユーザにより選択される。

一般に、平文データを暗号化データ生成手段１６により暗号化処理するためには、パスワードの設定が必要になる。パスワードは、先に説明したようにユーザが任意で設定した文字列を用いる。また、本実施の形態においては、暗号化処理されたデータの復号化処理の態様もユーザにより任意に設定されているので、光ディスク装置１０が、暗号化データの復号化処理の態様についてを区別するための補助パスワードが設定される。

【００２３】

補助パスワードは、工場出荷時において光ディスク装置１０に附されているシリアルナンバーや、機種名あるいは暗号化データの使用が許可されているグループ名等を設定し、あらかじめ第２の記憶手段２４に記憶させておくと共に、アプリケーション４２の選択ボタンに関連付けしておけば好適である。また、複数の補助パスワードを設定することも可能であり、ある補助パスワードは、工場出荷時に設定されていて、他の補助パスワードは、ユーザにより設定可能にしておけばさらに好適である。

これらにより、暗号化処理は、ユーザが設定した任意の文字列からなるパスワードに補助パスワードを組み合わせて鍵を形成し、暗号化データ生成手段１６によりなされることになるため、ユーザが設定したパスワードを入手したのみでは、暗号化データを復号処理させることができなくなり好適である。なお、補助パスワードを用いずにユーザが設定したパスワードのみで鍵を形成する形態としてもよいのはもちろんである。

このようにユーザの設定したパスワードに補助パスワードを付加させることが可能になっているので、ユーザにより設定されるパスワードはブランク（空白）のパスワードとし、補助パスワードのみの文字列を鍵を形成させることも十分に可能である。

【００２４】

暗号化データ生成手段１６は、所定のアルゴリズムにより平文データを暗号化する手段である。暗号化に関する所定のアルゴリズムとしては様々な規格が存在しているが、本実施の形態においては、ユーザにより設定された任意の文字列またはユーザにより設定された任意の文字列に補助パスワードを加えた文字列を鍵として暗号化処理する方式が用いられていて、例えば、秘密鍵暗号であるＤＥＳ方式等が挙げられるが、この暗号化方式に限定されるものではない。

暗号化データ生成手段１６において、アプリケーション４２上でユーザが設定したパスワード（ブランクのパスワードを含む）または、ユーザにより設定された任意の文字列に補助パスワードを加えた文字列を鍵として暗号化されたデータは、データ書き込み手段１８に送信された後、光ディスク３０に記録される。復号化手段２２は、少なくとも暗号化データ生成手段１６に対応したアルゴリズムが組み込まれているのは言うまでもない。

【００２５】

第１の実施の形態における光ディスク装置のデータ処理工程について説明する。図２は、第１の実施の形態におけるデータ処理工程の概略を示す説明図である。

パーソナルコンピュータ等の外部機器４０からアプリケーション４２を介して、平文データが光ディスク装置１０の第１の記憶手段１４に送られる（Ｓ１０１）。第１の記憶手段１４は送られた平文データを一時保管する（Ｓ１０２）。アプリケーション４２を介してユーザが平文データを暗号化処理するか否かを選択する（Ｓ１０３）。

ここで、暗号化処理が選択されなかった場合には、通常の手順によって光ディスク３０に平文データが書き込まれる。つまり、平文データがデータ書き込み手段１８に送信され、制御部１２により、データ書き込み手段１８が光ディスク３０に平文データを書き込む処理が実行される。

暗号化処理を選択した場合には、光ディスク装置１０に暗号化処理コマンドが送信される。ユーザは引き続きアプリケーション４２上で暗号化処理をしたデータの復号化処理の態様を選択する（Ｓ１０４）。

【００２６】

ユーザによりデータを暗号化処理する選択がなされた場合、アプリケーション４２を介して、ユーザがデータを暗号化処理する際に必要なパスワードが入力される（Ｓ１０５）。パスワードが入力されたら、制御部１２が、第２の記憶手段２４に記憶される復号化処理の態様を見分けるための補助パスワードをパスワードに付加する（Ｓ１０６）。制御部１２が第１の記憶手段１４に一時記憶されている平文データを読み出し（Ｓ１０７）、暗号化データ生成手段１６がパスワードと補助パスワードを合わせた文字列を鍵として平文データを暗号化処理する（Ｓ１０８）。その後、暗号化されたデータはデータ書き込み手段１８に送られ、データ書き込み手段１８によって光ディスク３０に記録される（Ｓ１０９）。

このようにして暗号化されたデータを復号する際は、暗号化データが記録されている光ディスク３０を光ディスク装置１０にセットした後、データ読み込み手段２０が光ディスク３０に書きこまれているデータを読み出し（Ｓ１１０）、第１の記憶手段１４にデータが一時記憶される（Ｓ１１１）。続いて、ユーザがデータを復号化するか否かを決定し（Ｓ１１２）、復号化処理をするならば、アプリケーション４２上から復号化の態様を選択する（Ｓ１１３）と共に、平文データを暗号化処理する際に設定したパスワードを入力し（Ｓ１１４）、さらに補助パスワードを付加する（Ｓ１１５）。

【００２７】

制御部１２は、第１の記憶手段１４に記憶されている光ディスク３０に記録されていた、暗号化処理されたデータをデータ読み込み手段２０に読み出させ（Ｓ１１６）、読み取った暗号化データを復号化手段２２に送信した後、復号化手段２２がアプリケーション４２を介してユーザにより設定されて入力されたパスワードに、同じくアプリケーション４２で選択された復号化態様に関連付けられている補助パスワードを付加した文字列より成る鍵を用いて復号処理を行う（Ｓ１１７）。パスワードが正しければ暗号化データは平文データに変換され、平文データが制御部１２を介してパーソナルコンピュータ等の外部機器４０へ送信され（Ｓ１１８）て、通常のデータとして使用することが可能になる。

反面、入力されたパスワードが正しくなければ、暗号化処理されたデータは正しいデータに変換されないため、パーソナルコンピュータ等の外部機器４０が変換されたデータを正しく読み取れないので、ファイルやデータを認識することができなくなる。

なお、復号化処理をしない選択をした場合には、特に何らの処理も行われないのは言うまでもない。

【００２８】

（第２の実施の形態）

第１の実施の形態においては、ユーザが設定したパスワードまたは、ユーザが設定したパスワードに復号化の態様に関連付けられた補助パスワードから成る文字列を鍵として暗号化および復号化処理を行う形態であるが、本実施の形態においては、第１の実施の形態における光ディスク装置１０にパスワード変換手段２６を追加することにより、平文データを暗号化し、暗号化処理されたデータの復号化処理を実行する際において、パスワードまたは、パスワードおよび補助パスワードから成る文字列を所定の関数により数値変換し、その数値を鍵として暗号化および復号化処理を行うことを特徴としている。

【００２９】

図３は第２の実施の形態における光ディスク装置１０の内部構成を示す説明図である。なお、本実施の形態において、第１の実施の形態と共通する構成要素については、第１の実施の形態と同じ符号を附すことにより、それらの要素についての詳細な説明は省略する。パスワード変換手段２６は、ユーザにより設定されたパスワードまたは、ユーザにより設定され入力されたパスワードおよび復号化形態に関連付けされている補助パスワードから成る文字列を数値化するための手段である。任意の文字列を数値化する手段としては様々

な形式のものが提供されているが、本実施の形態においては、ハッシュ関数を用いることにしている。ハッシュ関数は、一方向関数であるので、ハッシュ関数により得られた数値から元のパスワードを推測することは事実上不可能であるので、データ保護の安全性を向上させることができ、好適である。

【００３０】

第２の実施の形態における光ディスク装置のデータ処理工程について説明する。図４は、第２の実施の形態におけるデータ処理工程の概略を示す説明図である。

パーソナルコンピュータ等の外部機器４０から操作用入力手段であるアプリケーション４２を介して、平文データが光ディスク装置１０の第１の記憶手段１４に送られる（Ｓ２０１）。第１の記憶手段１４は送られた平文データを一時保管する（Ｓ２０２）。アプリケーション４２を介してユーザが平文データを暗号化処理するか否かを選択する（Ｓ２０３）。

ここで、暗号化処理が選択されなかった場合には、通常の手順によって光ディスク３０に平文データが書き込まれる。つまり、平文データがデータ書き込み手段１８に送信され、制御部１２により、データ書き込み手段１８が光ディスク３０に平文データを書き込む処理が実行される。

【００３１】

アプリケーション４２を介して、ユーザが光ディスク装置１０に暗号化処理をさせる選択をした場合、ユーザはアプリケーション４２を介して暗号化データの復号化処理の態様を選択し（Ｓ２０４）、アプリケーション４２を介して暗号化処理する際に必要なパスワードを入力する（Ｓ２０５）。パスワードが入力されたら、第２の記憶手段２４に記憶されている復号化処理の態様を見分けるための補助パスワードをパスワードに付加し（Ｓ２０６）、パスワード変換手段２６により数値に変換（ハッシュ化）される（Ｓ２０７）。制御部１２は、第２の記憶手段２４に一時記憶されている平文データを読み出し（Ｓ２０８）、暗号化データ生成手段１６は、パスワードを変換して得られた数値（ハッシュ値）を鍵として読み出された平文データを暗号化処理する（Ｓ２０９）。その後、暗号化したデータはデータ書き込み手段１８に送られ、データ書き込み手段１８によって光ディスク３０に記録される（Ｓ２１０）。

【００３２】

暗号化されたデータを復号する際は、暗号化データが記録されている光ディスク３０を本実施の形態における光ディスク装置１０にセットし、データ読み込み手段２０が暗号化データを読み取り（Ｓ２１１）、第１の記憶手段１４が読み出したデータを一時記憶する（Ｓ２１２）。ユーザがアプリケーション４２上から復号化の態様を選択する（Ｓ２１３）。復号化処理が選択された場合には、ユーザは引き続いて復号化態様を選択し（Ｓ２１４）、平文データを暗号化データ生成手段１６により暗号化処理する際に設定したパスワードを入力する（Ｓ２１５）。パスワード変換手段２６は、ユーザにより入力されたパスワードに複合化の態様に関連付けられている補助パスワードを付加する（Ｓ２１６）。制御部１２は、パスワード変換手段２６にパスワードと補助パスワードをまとめて数値に変換（ハッシュ化）させ（Ｓ２１７）ると共に、第１の記憶手段に記憶させてある暗号化データを読み出し（Ｓ２１８）、復号化手段２２にデータを送る。復号化手段２２はパスワードを変換して得られた数値（ハッシュ値）を鍵として暗号化データを復号処理する（Ｓ２１９）。入力されたパスワードが正しければ、パスワード変換手段２６により変換されて得られる数値（鍵）が一致するので、暗号化データは復号化手段２２により暗号化する前の状態（平文データ）に復号され、制御部１２を介して平文データがパーソナルコンピュータ等の外部機器４０に送信され（Ｓ２２０）、復号されたデータ（平文データ）に関連付けされているソフトウェアにより使用可能になる。

一方、Ｓ２１３において復号化処理をしない選択がなされた場合においては、特に何らの処理もなされることはない。

【００３３】

なお、ハッシュ値を第２の記憶手段２４に記憶させておけば、データ処理のたびにパスワ

ードを設定する必要を無くすことができる。このようにパスワードを第２の記憶手段２４に記憶させる形態は、限られたユーザのみが光ディスク装置にアクセスできる環境においては特に好適である。

【００３４】

以上、実施の形態に基いて本発明に係るデータ記録装置について詳細に説明してきたが、本発明はこれに限定されるものではない。したがって、本発明の要旨を変更しない範囲において各種の改変がなされたとしても本発明の技術範囲に属することは言うまでもない。例えば、暗号化および復号化形態の態様は、すべて光ディスク装置で暗号化、復号化処理する態様のみを想定しているが、データの暗号化および／または復号化を暗号化アプリケーションの態様に対応させるようにしてもよいのはもちろんである。これによれば、他の暗号化アプリケーションで暗号化等したデータを、実際に暗号化処理したアプリケーションなしでも復号処理等をすることができる。

【００３５】

また、本実施の形態においては、暗号化方式に秘密鍵暗号方式を採用しているが、公開鍵暗号方式を用いてもよいのはもちろんである。

さらには、補助パスワードは、必ずしも光ディスク装置に関する情報でなくても良く、ユーザにより任意に設定された文字列を第２の記憶手段に記憶させる形態としても良い。

【００３６】

また、操作用入力手段は、外部機器に設置したアプリケーションに限られることはなく、データ記録装置の本体に取り付けたものであってもよいのはもちろんである。

さらにまた、記録媒体は、固定式、リムーバブル式のいずれでもよく、光ディスクに限定されずに、固定ディスクや光磁気ディスクおよび磁気ディスク等を用いることももちろん可能である。

【００３７】

【発明の効果】

以上のことから、本発明におけるデータ記録装置を用いることにより以下に示す効果がある。

すなわち、本発明においては、記録装置自体に暗号化アルゴリズムが組み込まれていて、ユーザが任意のパスワードを設定することができるので、暗号化用アプリケーションを所有していなくても、手軽にデータを暗号化して記録媒体に記録することができる。

また、記録装置自体に復号化アルゴリズムが組み込まれていて、ユーザが任意のパスワードを設定することができるので、復号化用アプリケーションを所有していなくても、手軽に記録媒体に記録されている暗号化データを復号処理して使用することができる。

さらに、記録装置自体に暗号化アルゴリズムと復号化アルゴリズムが組み込まれていて、ユーザが任意のパスワードを設定することができるので、暗号化アルゴリズムや復号化用アプリケーションを所有していなくても、手軽に記録媒体に記録されている暗号化データを復号処理して使用することができる。

【００３８】

さらにまた、記憶手段には、ユーザにより設定されたパスワードに追加する補助パスワードがあらかじめ記憶されていることにより、暗号化したデータを復号化処理する際の属性を付加させることが可能になる。またさらには、暗号化したデータを復号化処理する際におけるデータの機密性を向上させることが可能になる。

また、ユーザが設定したパスワードと、複合化処理の属性に関連付けされた補助パスワードを記憶手段に記憶させるか否かを選択可能にしたことにより、たとえば、オフィスの同一グループ内での使用のように、何回も同じ条件で暗号化処理および復号化処理をする場合において、その都度パスワードの設定をする必要がなくなるため、データの機密性を維持しながらも記録装置の使用方法を簡素化することができる。

さらにまた、補助パスワードをデータ記録装置に関する情報とすることにより、補助パスワードによる属性を分かりやすくすることができる。

【００３９】

さらに、パスワードをハッシュ関数により ハッシュ化してから暗号化または復号化処理をすることにより、ユーザが設定したパスワードの長短によるパスワードの強度を均一のレベルにすることが可能になる。
また、ハッシュ値を記憶手段に記憶させることが可能に設定されているため、たとえば、オフィスの同一グループ内での使用のように、何回も同じ条件で暗号化処理および復号化処理をする場合において、その都度パスワードの設定をする必要がなくなるため、データの機密性を維持しながらも記録装置の使用方法を簡素化することができる。

【００４０】

さらに、前記記録媒体を、リムーバブルとしたことにより、データの供給先のデータ記録装置が共通していれば、該データ記録装置の設定を供給元のデータ記録装置の設定に合わせれば、暗号化したデータを復号することができるため、暗号化データの共有が容易になり、利便性が向上する等といった著効を奏する。

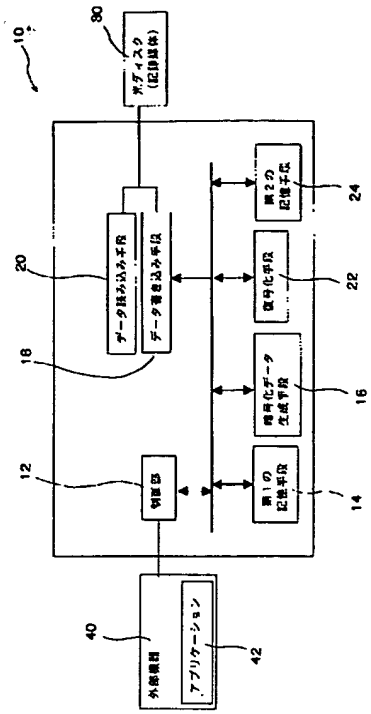
【図面の簡単な説明】

【図１】第１の実施の形態における光ディスク装置の構成を示す説明図である。
【図２】第１の実施の形態におけるデータ処理工程の概略を示す説明図である。
【図３】第２の実施の形態における光ディスク装置の構成を示す説明図である。
【図４】第３の実施の形態におけるデータ処理工程の概略を示す説明図である。

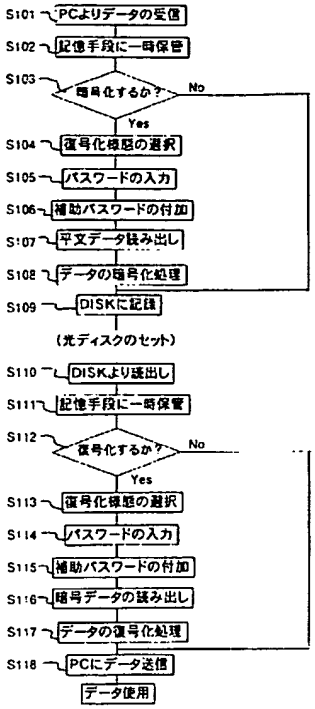
【符号の説明】

１０　記録装置
１２　制御部
１４　第１の記憶手段
１６　暗号化データ生成手段
１８　データ書き込み手段
２０　データ読み込み手段
２２　復号化手段
２４　第２の記憶手段
２６　パスワード変換手段
３０　光ディスク
４０　外部機器
４２　アプリケーション

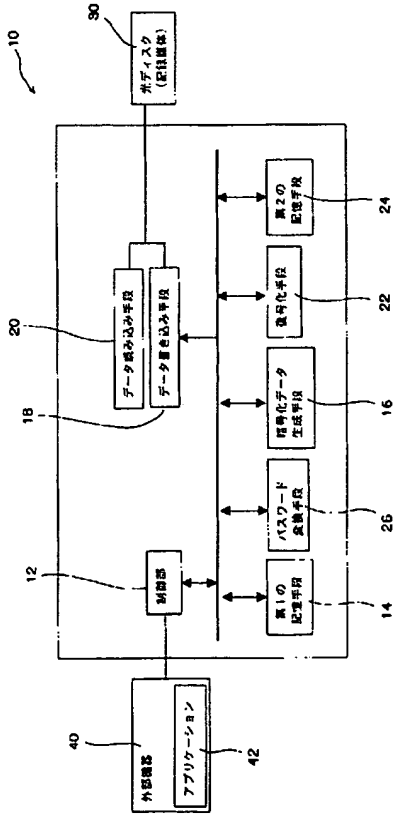
【図１】



【図２】



【図３】



【図４】